



UNITED STATES DISTRICT COURT  
FOR THE CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,  
  
Plaintiff,  
  
v.  
  
SHENGSHENG HE,  
aka "Adam,"  
  
Defendant.

CR No. 2:25-CR-00175-PA

I N F O R M A T I O N

[18 U.S.C. § 371: Conspiracy to  
Operate an Illegal Money  
Transmitting Business;  
18 U.S.C. § 982: Criminal  
Forfeiture]

The Acting United States Attorney charges:

COUNT ONE

[18 U.S.C. § 371]

A. INTRODUCTORY ALLEGATIONS

At times relevant to this Information:

1. Defendant SHENGSHENG HE ("HE"), also known as ("aka")  
"Adam," was a citizen of the United States and resided in Los  
Angeles, California, and Mexico City, Mexico.

2. Co-Conspirator 1 was a citizen of the United States and resided in Los Angeles, California.

3. Co-Conspirator 2 was a citizen of the People's Republic of China ("PRC") and resided in the United Arab Emirates.

4. Co-Conspirator 3 was a citizen of the PRC and St. Kitts and Nevis and resided in the Kingdom of Cambodia, the United Arab Emirates, and the PRC.

5. Axis Digital Limited ("Axis Digital") was an entity incorporated under the laws of the Commonwealth of the Bahamas on or about November 30, 2021.

6. "Bahamas Account #1" was an account at Deltec Bank and Trust Limited ("Deltec Bank") in the Bahamas, opened by Axis Digital on or about February 25, 2022.

7. B&C Commerce LLC ("B&C Commerce") was a shell company registered with the California Secretary of State on or about January 21, 2022, with a principal address in San Gabriel, California.

8. Jimei Trading Inc. ("Jimei Trading") was a shell company registered with the California Secretary of State on or about May 15, 2022, with a principal address in San Gabriel, California.

9. YXJ Trading Corporation ("YXJ Trading") was a shell company registered with the California Secretary of State on or about July 30, 2022, with a principal address in Monterey Park, California.

10. YYJ Consulting Corporation ("YYJ Consulting") was a shell company registered with the California Secretary of State on or about August 25, 2022, with a principal address in Monterey Park, California.

11. Sea Dragon Trading, LLC ("Sea Dragon Trading") was a shell company registered with the California Secretary of State on or about

1 September 8, 2022, with a principal address in Alhambra, California.

2 12. SMX Beauty Inc. ("SMX Beauty") was a shell company  
3 registered with the California Secretary of State on or about October  
4 13, 2022, with a principal address in Monterey Park, California.

5 13. SMX Travel Inc. ("SMX Travel") was a shell company  
6 registered with the California Secretary of State on or about October  
7 13, 2022, with a principal address in Monterey Park, California.

8 14. Sea Dragon Remodel, Inc. ("Sea Dragon Remodel") was a shell  
9 company registered with the California Secretary of State on or about  
10 October 17, 2022, with a principal address in Vernon, California.

11 15. The virtual-currency wallet address beginning with TRteo  
12 (the "TRteo Address") was a wallet that received transfers of virtual  
13 currency converted from funds in Bahamas Account #1.

14 B. DEFINITIONS

15 16. "Digital currency" or "virtual currency" is currency that  
16 exists only in digital form; it has some of the characteristics of  
17 traditional money, but it does not have a physical equivalent.  
18 Cryptocurrency, a type of virtual currency, is a network-based medium  
19 of value or exchange that may be used as a substitute for traditional  
20 currency to buy goods or services or exchanged for traditional  
21 currency or other cryptocurrencies. USDT, or Tether, is a virtual  
22 currency whose value is pegged to the U.S. dollar.

23 17. The term "spoofed" refers to domain spoofing, a process by  
24 which cybercriminals seek to persuade victims that a web address or  
25 email belongs to a legitimate and generally trusted company, when in  
26 fact it links the user to a fraudulent site controlled by a  
27 cybercriminal.

28 18. In "pig butchering" fraud schemes (a term derived from a

foreign-language phrase used to describe these crimes), scammers encounter victims on dating services, social media, or through unsolicited messages or calls, often masquerading as a wrong number. Scammers initiate relationships with victims and slowly gain their trust, eventually introducing the idea of making a business investment using cryptocurrency. Victims are then directed to other members of the scheme operating fraudulent cryptocurrency investment platforms and applications, where victims are persuaded to make financial investments. Once funds are sent to scammer-controlled accounts, the investment platform often falsely shows significant gains on the purported investment, and the victims are thus induced to make additional investments. Ultimately, the victims are unable to withdraw or recover their money, often resulting in significant losses for the victims.

19. In "customer service" or "tech support" fraud schemes, victims are contacted by fake customer service or technology support representatives. Scammers often pretend to represent a prominent company and contact the victim to alert them to a supposed infection with a computer virus or false issue with the victim's computer or other digital device. Scammers then take a variety of actions to defraud the victim, including, but not limited to, the following: (a) causing the victim to provide them with remote access to the victim's digital devices to supposedly remediate the problem, (b) requesting that funds be transferred to pay for assistance, and (c) advising the victim to transfer money from accounts that are supposedly compromised by the problem to accounts controlled by the scammer.

C. OBJECT OF THE CONSPIRACY

20. Beginning on an unknown date, but no later than on or about

1 November 2021, and continuing to in or about July 2023, in Los  
2 Angeles County, within the Central District of California, and  
3 elsewhere, defendant HE, with others known and unknown, knowingly  
4 conspired and agreed to commit an offense against the United States,  
5 namely, to operate an unlicensed money transmitting business, in  
6 violation of 18 U.S.C. §§ 1960(b)(1)(B) and 1960(b)(1)(C).

7 D. THE MANNER AND MEANS OF THE CONSPIRACY

8 21. The object of the conspiracy was to be accomplished in  
9 substance as follows:

10 Solicitation of Investment Fraud Victims

11 a. Unindicted co-conspirators would contact victims  
12 directly through unsolicited social-media interactions, telephone  
13 calls and messages, and online dating services.

14 b. Unindicted co-conspirators would gain the trust of  
15 victims by establishing either professional or romantic relationships  
16 with the victims. Unindicted co-conspirators would build these  
17 relationships through interstate communications, including, but not  
18 limited to, electronic messages sent via end-to-end encrypted  
19 applications.

20 c. Unindicted co-conspirators would promote fraudulent  
21 cryptocurrency investments to the victims after gaining the victims'  
22 trust.

23 d. Unindicted co-conspirators would establish spoofed  
24 domains and websites that resembled legitimate cryptocurrency trading  
25 platforms.

26 e. In some executions of the scheme, unindicted co-  
27 conspirators would fraudulently induce victims into investing in  
28 cryptocurrency through these fraudulent and spoofed investment

1 platforms.

2 f. In other executions of the scheme, unindicted co-  
3 conspirators would fraudulently induce victims into investing in  
4 cryptocurrency by sending funds via wire transfer.

5 g. Unindicted co-conspirators would fraudulently  
6 represent to victims that the victims' investments were appreciating  
7 when, in fact, those funds had been converted by members of the fraud  
8 scheme.

9 Solicitation of Customer Service and Tech Support Fraud Victims

10 h. Unindicted co-conspirators would fraudulently  
11 represent to victims through interstate communications, including,  
12 but not limited to, electronic messages and phone calls, that they  
13 were from a customer service or technology support company.

14 i. Unindicted co-conspirators would fraudulently induce  
15 victims to send funds via wire transfer or cryptocurrency trading  
16 platforms to purportedly remediate a non-existent virus or other  
17 false computer-related problem.

18 Operation of Unlicensed Money Transmitting Business

19 j. Co-conspirators would register dozens of U.S. shell  
20 companies with the California Secretary of State and elsewhere,  
21 including B&C Commerce, Jimei Trading, YXJ Trading, YYJ Consulting,  
22 SMX Beauty, SMX Travel, Sea Dragon Trading, and Sea Dragon Remodel.

23 k. Co-conspirators would open bank accounts in the names  
24 of various shell companies.

25 l. Co-conspirators would receive victim funds in U.S.  
26 bank accounts established on behalf of shell companies and cause the  
27 further transfer of victim funds to domestic and international bank  
28 accounts.

1 m. Defendant HE and co-conspirators would monitor the  
2 receipt and execution of interstate and international wire transfers  
3 of victim funds, including to Bahamas Account #1.

4 n. Defendant HE and other co-conspirators would monitor  
5 the conversion of victim funds to USDT and the subsequent  
6 distribution of virtual currency to cryptocurrency wallets.

7 o. Defendant HE and co-conspirators would direct the  
8 conversion of nearly all of the funds into USDT and the subsequent  
9 transfer of cryptocurrency to the TRteo Address.

10 p. Defendant HE would receive a commission for the  
11 transfer of victim funds to USDT and would distribute ledgers  
12 detailing the profit-sharing arrangement.

13 q. Defendant HE and other co-conspirators would possess  
14 fraudulent "Know Your Customer" ("KYC") documents associated with  
15 these wire transfers.

16 r. Co-conspirators would cause wire transfers to be sent  
17 through various intermediary bank accounts before reaching their  
18 final beneficiary.

19 s. Defendant HE would receive victim funds in financial  
20 accounts he directly controlled.

21 t. Defendant HE and other co-conspirators would  
22 communicate with each other and coordinate acts in furtherance of the  
23 conspiracy through encrypted messaging services.

24 E. OVERT ACTS

25 22. In furtherance of the conspiracy and to accomplish its  
26 object, defendant HE, Co-Conspirators 1, 2, and 3, and others known  
27 and unknown, on or about the dates set forth below, committed and  
28 caused to be committed various overt acts, in the Central District of

1 California and elsewhere, including, but not limited to, the  
2 following:

3 Overt Act No. 1: On November 30, 2021, Co-Conspirator 1,  
4 defendant HE, and other co-conspirators established the Bahamian  
5 entity Axis Digital.

6 Overt Act No. 2: On June 8, 2022, defendant HE sent messages  
7 in an encrypted messaging platform introducing several co-  
8 conspirators to each other and discussing the transfer of funds to  
9 Co-Conspirator 1 to open Bahamas Account #1, including a video of Co-  
10 Conspirator 1's financial account.

11 Overt Act No. 3: On July 6, 2022, defendant HE traveled to  
12 Phnom Penh, Cambodia, to meet with co-conspirators regarding the  
13 operation of Bahamas Account #1 and the transfer of USDT to the TRTeo  
14 Address.

15 Overt Act No. 4: On July 6, 2022, defendant HE sent a message  
16 in an encrypted messaging platform to Co-Conspirator 3 regarding  
17 communications with Deltec Bank employees.

18 Overt Act No. 5: On July 6, 2022, defendant HE sent via an  
19 encrypted messaging platform a template for the "Know Your Customer"  
20 document associated with Axis Digital and the conversion of funds in  
21 Bahamas Account #1 to USDT.

22 Overt Act No. 6: On an unknown date but no later than July 7,  
23 2022, defendant HE corresponded with a Deltec Bank employee who acted  
24 as the account manager for Bahamas Account #1 regarding the  
25 conversion of funds to USDT.

26 Overt Act No. 7: On August 5, 2022, defendant HE corresponded  
27 with Deltec Bank employees on an encrypted messaging platform and  
28 confirmed that funds from Bahamas Account #1 should be converted to



1 USDT and transferred to the TRteo Address.

2 Overt Act No. 8: On an unknown date but no later than  
3 September 28, 2022, defendant HE sent Deltec Bank employees wire  
4 forms associated with transfers to Bahamas Account #1 from YYJ  
5 Consulting and YXJ Trading.

6 Overt Act No. 9: On November 14, 2022, defendant HE messaged  
7 co-conspirators stating that, "Starting this time, the three of us  
8 have the same ratio of 20/20/20."

9 Overt Act No. 10: On November 16, 2022, defendant HE received,  
10 in a U.S. bank account he directly controlled, approximately \$150,000  
11 from a shell company that received victim funds from a cryptocurrency  
12 investment scam.

FORFEITURE ALLEGATION

[18 U.S.C. § 982]

1. Pursuant to Rule 32.2(a) of the Federal Rules of Criminal Procedure, notice is hereby given that the United States of America will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Section 982(a)(2), in the event of defendant's conviction of the offense set forth in this Information.

2. Defendant, if so convicted, shall forfeit to the United States of America the following:

(a) All right, title and interest in any and all property, real or personal, constituting, or derived from, any proceeds obtained, directly or indirectly, as a result of the offense; and

(b) To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraph (a).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b), defendant, if so convicted, shall forfeit substitute property, up to the total value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph, or any portion thereof: (a) cannot be located upon the exercise of due diligence; (b) has been transferred, sold to or deposited with a third party; (c) has been placed beyond the jurisdiction of the court; (d) has been

//

//

//

substantially diminished in value; or (e) has been commingled with  
other property that cannot be divided without difficulty.

JOSEPH T. MCNALLY  
Acting United States Attorney



DAVID T. RYAN  
Assistant United States Attorney  
Chief, National Security Division

KHALDOUN SHOBAKI  
Assistant United States Attorney  
Chief, Cyber & Intellectual Property  
Crimes Section

MAXWELL COLL  
ALEXANDER S. GORIN  
Assistant United States Attorneys  
Cyber & Intellectual Property Crimes  
Section

NISHA CHANDRAN  
Assistant United States Attorney  
Corporate and Securities Strike  
Force

STEFANIE SCHWARTZ  
TAMARA LIVSHIZ  
Trial Attorneys  
National Cryptocurrency Enforcement  
Team  
Computer Crime & Intellectual  
Property Section